FOUNDED 1870

AMERICAN CORRECTIONAL ASSOCIATION

206 NORTH WASHINGTON STREET, SUITE 200 • ALEXANDRIA, VIRGINIA 22314
703 • 224 • 0000 FAX: 703 • 224 • 0010
WWW.ACA.ORG

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: American Correctional Association Comments on Combating Contraband Wireless Device Use in Correctional Facilities, GN Docket No. 13-111; FCC 17-25

Dear Ms. Dortch:

The American Correctional Association (ACA) respectfully submits these comments in response to the Commission's May 18, 2017 request for additional comments in the above-referenced rulemaking proceeding.

ACA is vitally concerned, as a matter of life and death for our members and as a matter of public safety, in the Federal Communications Commission (FCC) finally crafting a technological solution to defeat contraband cell phones in correctional facilities. ***We state emphatically that a technological solution exists*** if the FCC is able to view this as a public safety matter that trumps the FCC's traditional modes of operation. We congratulate the FCC for its work in this area and for the Further Notice of Proposed Rulemaking, but we must insist that you use your utmost efforts to implement a system that employs existing technology to protect the public and our members from contraband cell phones.

ACA is a professional membership organization composed of individuals, agencies and organizations involved in all facets of the corrections field, including adult and juvenile services, community corrections, probation and parole and jails. It has approximately 20,000 members in the United States, Canada and other nations, as well as 100 chapters and affiliates representing states, professional specialties, or university criminal justice programs. For nearly 140 years, the ACA has been the driving force in establishing national correctional policies and advocating safe, humane and effective correctional operations. Today, the ACA is the world-wide authority on correctional policy and standards, disseminating the latest information and advances to members, policymakers, individual correctional workers and departments of correction.

Contraband cell phones pose an extremely serious and proven threat to the safety of staff and inmates and to the overall security of the facility. Correctional facility administrators, wardens and staff should have the best technology and toolset available to them to combat this illicit cell phone use. Possessing a cell phone inside of correctional facility is a criminal offense in the federal bureau of

prisons and in most states. The number of phones being smuggled into correctional facilities is on the rise and is becoming a greater and greater challenge every day. Likewise, the resources and efforts required to combat contraband cell phones is becoming burdensome for corrections. Even worse, they can and are being used to circumvent facility security and authority, to conduct criminal enterprises on the outside, commit murder and other crimes and to threaten witnesses. The reports of inmates running criminal enterprises from inside of prisons using contraband cell phones continue to increase. Cryptocurrencies now give inmates a nearly untraceable means to launder money and encryption software programs make the devices unintelligible even when they are discovered.

The number of confiscated cell phones within the state correctional systems and the Federal Bureau of Prisons is on the rise. Consequently, this persistent problem poses a very serious and growing threat to facility security and employee, inmate and public safety. We believe that coordinated and well-developed plans can mitigate this problem through the use of the best technologies available to us.

ACA appreciates the work that the FCC has done to facilitate one kind of technology in the current rulemaking, Managed Access Systems (MAS). However, MAS is not fool-proof and is far too expensive for most correctional facilities. ACA strongly recommends that any technology implemented to address this problem meet all of the following required criteria:

1. **Render unusable.** The technology must be able to completely render the wireless device unusable, with the possible exception of 9-1-1, preventing all other voice calls, data usage, memory function, photography or any other function or application that can be used to transmit or record any form of communications, even by passing the device physically.

2. **Ubiquity and interoperability.** The technology must work on all wireless devices for all carriers. It must work throughout the facility, which has been a problem for jammers and MAS.

3. **Cost-effectiveness.** The technology must be affordable for all correctional facilities, which has been a problem for MAS and some of the other proposed technologies. The technology must be flexible enough to be updated without undue expense or the expenditure of capital funds to keep the capabilities functional. The best technology is useless if it is unaffordable.

4. **Non-interference.** The technology must not interfere with communications signals outside the correctional facility, which has been a problem with jammers and MAS.

5. **Ease of operation.** The technology must work quickly and almost automatically without significant human intervention, from either correctional personnel, carrier personnel or contractors. It should not require much supervision, oversight or manual input to disable the device. The system should

ideally work passively and automatically. MAS requires a great deal of human activity and time, as does some of the detection systems.

6. **Secure.** The technology must be secure from tampering or interference by inmates or any non-authorized personnel and it must have strong protections against breaches in cybersecurity from hacking or disruption.

7. **Compliant.** The technology must be legal and compliant with state and federal law and with the regulations of the FCC.

ACA does not endorse any one product or company over any other. The ACA advocates for use and implementation of the best technology to effectively combat and put an end to this devastating public safety crisis. The FCC should not take any action that would limit a correctional facility in choosing solutions, whether those are MAS, detection systems or other legal options.

However, the FCC must recognize that to achieve the required criteria listed above, the FCC must take proactive action. ACA has reviewed the available technologies and finds that continuous wave beacon technology (CW beacon systems) meets all of the requirements and is especially attractive because it is cost-effective and does not require a huge capital expense. This technology is now available, but it requires the cooperation of carriers and manufacturers to implement, something only the FCC can secure.

The ACA believes that continuous wave beacon technology, which is specifically called out for comment in paragraphs 131 and 132 of the March 23 NPRM, incorporates all of these features. CW beacon systems operate without interference with any cellular network frequencies, do not require human intervention by either corrections personnel or carrier personnel and can shut down ***all functions*** of the cell phone as soon as it picks up the signal from the beacon.

Carrier and cell phone manufacturer involvement would be limited to an initial push of the beacon technology onto cell phones on each carrier's respective network. After that, the continuous wave beacon technology would operate without any further involvement from the carrier or cell phone manufacturer, and could be automatically updated ensuring forward compatibility in the future.

Anyone that tries to move or tamper with the beacon will render it unusable; tampering or moving causes its software to be wiped so that it cannot be reverse engineered. The cost of the beacons is minimal compared to every other system proposed for combating contraband cell phones.

While ACA has supported the use of Managed Access Systems, having seen some of the problems with implementation, effectiveness, cost and issues with overbreadth and gaps, we would discourage the Commission from viewing managed access as the best solution or final solution to solving this problem. MAS systems have their limitations and are very expensive to implement on a broad scale. The process by which carriers receive and process requests for termination of services is slow and therefore not an effective solution (this goes to the ACA required criterion of ease of operation). Furthermore, the application process for spectrum lease

agreements required for MAS is often slow and inefficient, even with the FCC's proposed changes. More importantly, MAS does not necessarily disable all functions of a contraband cell phone that can be used to communicate with others. Certain functions (*e.g.*, camera usage and, potentially, internet access) may still be used by inmates.

Jamming systems can be over-inclusive and interfere with legitimate wireless devices in the surrounding areas. ACA has supported jamming systems, but it is our understanding that the FCC's position remains that jamming is banned statutorily. As with MAS, jamming systems still permit inmates to use certain functions on a contraband cell phone.

Another approach, Geolocation-Based Denial, is a system wherein correctional administrators can petition the Commission to declare correctional facilities outside of the authorized service area of all CMRS carriers if that said facility meets certain specific criteria, such as 300 meters of space in all directions. This approach puts more of the impetus on carrier expertise and technologies, rather than the taxpayers and/ or budget- restricted public safety agencies. But this approach has limitations as well, for example, the cell phone is still able to be operated even when not connected to the network. To effectively end the serious problem of contraband cell phone use, the technology must be able to meet the ACA required criterion of completely shutting down all functions of the device.

Put simply, while these other systems discussed above can be effective in some instances, they are not without their complications, they are not cost-effective for all correctional institutions and they do not meet all of the ACA's required criteria listed above.

Traditionally, the FCC has not specified technologies, leaving the selection to the marketplace. Such a concept is totally inappropriate to the public safety setting, and in fact, the failure of the market to arrive at a meaningful solution over the decades in which cell phones have been in use is strong evidence that the FCC's 'technology neutral' approach has not worked. Indeed, the FCC has made exceptions for specifying technology where public safety is at stake, such as the FCC's designation of LTE for the national public safety broadband network, FirstNet. The dire situation with regard to contraband cell phones is directly analogous: the public safety demands a technological solution that spans all carriers and devices.

However, the FCC does not need to mandate the technology. We strongly encourage Chairman Pai to invoke his leadership role as a convener to gather the carriers and reach a voluntary agreement within one year to implement and offer CW beacon systems on all cell phones with a phase-in period of two years from the date of the agreement. A great example and precedent for such an action is the FCC's work as a convener to get the carriers to implement wireless emergency alerts on all cell phones voluntarily under the auspices of the Warning, Alert and Response Network Act (the WARN Act).

However, if all carriers do not agree within the one-year period, we would encourage the FCC to pursue mandatory requirements in this proceeding. This

issue merits such action by the FCC if the industry is not able to reach a solution when the technology exists to meet all of the ACA's required criteria.

While ACA believes that the best and quickest solution is for a voluntary program, the FCC does possess actual regulatory authority over the manufacturers under the FCC's Part 15 authority, and over the carriers under Section 332, Part 15 Ancillary Authority. The FCC has broad authority under Section 332 to regulate the spectrum over which wireless devices operate in order to promote the safety of life and property. More specifically, 47 U.S.C. § 332 provides, in pertinent part, "[i]n taking actions to manage the spectrum to be made available for use by the private mobile service, the Commission shall consider, consistent with section 1 of this Act, whether such actions will ... promote the safety of life and property." 47 U.S.C. § 332(a)(l).

ACA is willing to assist in facilitating the discussion of reaching a voluntary solution for CW beacon systems. We believe that it will require a united effort on the part of the federal government, state and local correctional agencies and professionals, cellular carriers, technology companies and victims' advocates. Only with the cooperation of each and every stakeholder will we be able to move forward and find solutions, but the most important part is for the FCC to take leadership and work with the carriers to achieve the voluntary program. In doing so, the FCC will have achieved a major accomplishment in fulfilling its statutory responsibility to public safety, striking a mighty blow against crime and earning the undying gratitude of all law enforcement officials, especially correctional officials.

Respectfully,

Lannette C. Linthicum, President
American Correctional Association

James A. Gondles, Jr., Executive Director
American Correctional Association